Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

Andrea Nicté Vicente Campos
Asesorado por Ing. Álvaro Giovanni Longo Morales

Guatemala, agosto 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ANDREA NICTÉ VICENTE CAMPOS
ASESORADO POR ING. ÁLVARO GIOVANNI LONGO MORALES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANA	Inga. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir ArmaCruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADORA	Inga. Floriza Felipa Avila Pesquera de Medinilla
EXAMINADOR	Ing. Sergio Leonel Gómez Bravo
EXAMINADOR	Ing. Carlos Alfredo Azurdia Morales
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas con fecha 5 de agosto de 2021.

Andrea Nicté Vicente Campos

Guatemala 20 de mayo de 2022

Ing. Oscar Argueta Hernández
Director de la Unidad de EPS
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Respetable Ing. Argueta:

Respetuosamente me dirijo a usted deseándole éxito en sus actividades cotidianas, por medio de la presente hago de su conocimiento que la estudiante Andrea Nicté Vicente Campos, quien se identifica con CUI No. 2924733621101 y como estudiante universitario con número de carné 201404104, ha finalizado el informe final del proyecto EPS:

"SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA"

Agradeciendo la atención a la presente y quedando a sus órdenes para cualquier información adicional.

Sin otro particular me suscribo, atentamente,

F:_____

Ing. Álvaro Giovanni Longo Morales
longoalvarousac@gmail.com

Alvaro Giovanni Longo Morales
Ingeniero en Ciencias y Sistemas
Colegiado No. 15,845

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Unidad de EPS

Guatemala, 26 de mayo de 2022.
REF.EPS.DOC.218.05.2022.

Ing. Oscar Argueta Hernández
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Argueta Hernández:

Por este medio atentamente le informo que como Supervisora de la Práctica del Ejercicio Profesional Supervisado, (E.P.S) de la estudiante universitaria de la Carrera de Ingeniería en Ciencias y Sistemas, **Andrea Nicte Vicente Campos, Registro Académico 201404101 y CUI 2924 73362 1101** procedí a revisar el informe final, cuyo título es **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA.**

En tal virtud, **LO DOY POR APROBADO**, solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Inga. Floriza Felipa Ávila Pesquera de Medinilla
Supervisora de EPS
Área de Ingeniería en Ciencias y Sistemas

FFAPdM/RA

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala 1 de junio de 2022

Ingeniero
Carlos Gustavo Alonzo
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Alonzo:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación-EPS de la estudiante **ANDREA NICTE VICENTE CAMPOS** carné **201404101** y CUI **2924 73362 1101,** titulado: **"SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA."** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

Universidad de San Carlos de Guatemala

Facultad de Ingeniería
Unidad de EPS

Guatemala, 26 de mayo de 2022.
REF.EPS.D.180.05.2022.

Ing. Carlos Gustavo Alonzo
Director Escuela de Ingeniería Ciencias y Sistemas
Facultad de Ingeniería
Presente

Estimado Ingeniero Alonzo:

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES EN DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA,** que fue desarrollado por la estudiante universitaria **Andrea Nicte Vicente Campos, Registro Académico 201404101 y CUI 2924 73362 1101** quien fue debidamente asesorada por el Ing. Álvaro Giovanni Longo Morales y supervisada por la Inga. Floriza Felipa Ávila Pesquera de Medinilla.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y la Supervisora de EPS, en mi calidad de Director apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

Ing. Oscar Argueta Hernández
Director Unidad de EPS

/ra

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

LNG.DIRECTOR.163.EICCSS.2022

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador de área y la aprobación del área de lingüística del trabajo de graduación titulado: **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA**, presentado por: **Andrea Nicté Vicente Campos**,procedo con el Aval del mismo, ya que cumple con los requisitos normados porla Facultad de Ingeniería.

"ID Y ENSEÑAD A TODOS"

Msc. Ing. Carlos Gustavo Alonzo
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, agosto de 2022

Decanato
Facultad de Ingeniería
24189101- 24189102
secretariadecanato@ingenieria.usac.edu.gt

LNG.DECANATO.OI.582.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al Trabajo de Graduación titulado: **SISTEMA DE INICIO DE SESIÓN ÚNICO PARA APLICACIONES DEL DEPARTAMENTO TÉCNICO CIENTÍFICO DEL INSTITUTO DE CIENCIAS FORENSES DE GUATEMALA,** presentado por: **Andrea Nicté Vicente Campos,** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANA
FACULTAD DE INGENIERÍA

Inga. Aurelia Anabela Cordova Estrada
Decana

Guatemala, agosto de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios	Por guiar mi camino, por alcanzar una de las metas más importantes de mi vida.
Mis padres	Efrén Ubaldo, Vicente Lorenzo y Sara Gladys Campos Calderón, por su apoyo incondicional.
Mi hermano	Andrés Alexander Vicente Campos, por estar conmigo en los días que había que dar un esfuerzo extra.
Mis abuelos	Arnulfo Vicente (q. e. p. d.), Fermina Lorenzo (q. e. p. d.) y Olga Calderón por animarme a seguir mis sueños.

AGRADECIMIENTOS A:

Mis amigos Tikiram Ruiz, Ingeborg Ortega, Sharolin Lacunza, Javier Chacón, Gabriela Contreras, Jorge Salazar, Tanya Muhun, Mauro Herrera, Luis Azurdia y Roberth Vásquez por el apoyo durante toda la carrera.

Mis tíos Imelda Vicente y Hugo Vicente, por ser guías importantes durante esta etapa de mi vida.

Ingenieros Irvin García, Willy Rosal y Álvaro Longo por el constante apoyo durante el desarrollo de mi proyecto de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
$	Dólar
Gb	*Gibabyte*
Mb	*Megabyte*
Q	Quetzal

GLOSARIO

Active Directory	Es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red, que necesitan para realizar su trabajo.
Backend	Parte del desarrollo web que se encarga de toda la lógica de una página web para que esta funcione.
Base de Datos	Recopilación organizada de información o datos estructurados, que se almacenan de forma electrónica en un sistema informático.
EPS	Ejercicio de práctica supervisada.
Implementación	Hace referencia a la aplicación puesta en marcha.
Integración	Resultado de mantener unidas las partes de un todo.
Json	*JavaScript Object Notation*, notación de objetos de *JavaScript*, formato ligero de intercambio de datos, que resulta sencillo de leer y escribir para programadores.

JWT	JSON *Web Token*, estándar que define un mecanismo para propagar entre dos partes de forma segura, la identidad de un determinado usuario, además de privilegios.
LDAP	*Lightweight Directory Access Protocol*. Es un protocolo de *software* que permite a cualquier persona localizar datos sobre organizaciones, personas y otros recursos en una red, pública o privado.
Log in	Proceso que controla el acceso individual a un sistema informático mediante la identificación de un usuario.
Log out	Proceso que termina la conexión de un usuario en un sistema informático.
OAuth2.0	Protocolo estándar de la industria para la autorización, proporciona flujos de autorización para aplicaciones web, de escritorios y también móviles.
OIDC	*OpenID Connect***,** protocolo de autenticación basado en Oauth 2.0, que se puede utilizar para que un usuario inicie sesión de forma segura en una aplicación, amplia el protocolo Oauth2.0, para usarlo como protocolo de autenticación, lo que permite realizar inicios de sesiones únicos mediante OAuth. Es una reescritura de SAML usando OAuth 2.0.

REST API	También conocido como RESTful API, es una interfaz de aplicación de programación. Permite interacción a servicios web RESTFul.
SAML	*Security Assertion Markup Language*. Es un estándar abierto que se utiliza para la autenticación basado en lenguaje XML.
SSO	*Single sign-on*, inicio de sesión único, permite a un usuario iniciar sesión con un solo ID, en varios sistemas.
Token	Es una colección de datos o información que se pasa de un sistema a otro durante todo el proceso de inicio de sesión único.
XHTML	*Extensive Hypertext Markup Language*. Es un tipo de lenguaje marcado que permite editar sitios web.

RESUMEN

Derivado de la necesidad de hacer uso de sistemas de información, la Unidad de Informática, como ente rector en el desarrollo de sistemas de información del Instituto Nacional de Ciencias Forenses de Guatemala, ha desarrollado varias aplicaciones, toma como punto de arranque los diferentes requerimientos de usuario. Durante esta fase de crecimiento de sistemas de información, no se tomó en cuenta el hacer uso de un sistema de inicio de sesión único a los usuarios, esto tuvo como impacto el tener que registrar a un usuario con credenciales específicas por cada sistema de información existente, en otras palabras, una persona podría tener hasta 5 usuarios diferentes para cada sistema de información existente.

Este proyecto de Ejercicio Profesional Supervisado (EPS) busca crear un mecanismo que permita centralizar el inicio de sesión de los usuarios, para que estos solo con una única credencial de usuario puedan ingresar a varios sistemas de información, restringiendo en los que estos se encuentren registrados. El proyecto facilitará el desarrollo de futuros sistemas de información desarrollados en la Unidad de Informática, para que puedan crearse sobre la base de un sistema de inicio de sesión único.

Este proyecto consiste en implementar una tercera solución que maneje los inicios de sesión únicos, para sistemas de información basados en la web del Instituto Nacional de Ciencias Forenses de Guatemala.

OBJETIVOS

General

Implementar un sistema de inicio de sesión único que permita el acceso a los sistemas de información basados en la web del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses de Guatemala.

Específicos

1. Implementar *Keycloak* como un *software* de tercero que controle el inicio de sesión único en los sistemas de información basados en la web.

2. Establecer un sistema, para que los nuevos sistemas de información basados en la web del Instituto Nacional de Ciencias Forenses de Guatemala puedan ser desarrollados con un inicio de sesión único.

3. Integrar en los sistemas de información basados en la web ya existentes del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses de Guatemala en el sistema de inicio de sesión único.

INTRODUCCIÓN

Actualmente, el Instituto Nacional de Investigación de Ciencias Forenses, cuenta con múltiples sistemas de información basados en la web, desarrollados con diferentes tecnologías, la cantidad de estos se ha ido incrementando y lo seguirán haciendo, por lo que se busca una solución para unificar todos los sistemas actuales y por existir en un único sistema de autenticación, y con ello evitar tener un usuario y contraseña diferente para cada plataforma, ya que dicho de otra manera una persona puede llegar a tener 10 usuarios diferentes, con credenciales propia de cada plataforma, lo cual a una proyección futura, esto puede ser un gran inconveniente, por lo que se formula la presente propuesta de este proyecto.

Bajo en contexto anterior, se implementará un *software* de tercero, que tiene el nombre *Keycloak*, para manejar las sesiones de los usuarios, creando un sistema de inicio de único sobre los servicios que provee *Keycloak*, se busca que los sistemas de información basados en la web que se estén desarrollando actualmente o en un futuro sean creados sobre la base de un inicio de sesión único, y que los sistemas de información basados en la web ya existentes del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses de Guatemala, se integren a este sistema.

1. FASE DE INVESTIGACIÓN

1.1. Antecedentes de la empresa

El Instituto Nacional de Ciencias Forenses de Guatemala surge de la necesidad de contar con un ente auxiliar al sector justicia, capaz de unificar los servicios forenses periciales y garantizar la imparcialidad y confiabilidad de la investigación técnica científica. Desde su creación, y desde la perspectiva tecnológica, se han realizado esfuerzos para contribuir con el propósito institucional, donde se incluyen: equipar con equipo de cómputo a las diferentes dependencias del INACIF, crear una infraestructura de red institucional y automatizar diferentes procesos mediante la implementación de una serie de herramientas de *software* que son de propósito específico.

1.1.1. Reseña histórica

El Instituto Nacional de Ciencias Forenses de Guatemala surge de la necesidad de contar con un ente auxiliar al sector justicia, capaz de unificar los servicios forenses periciales y garantizar la imparcialidad y confiabilidad de la investigación técnica científica.

Desde su creación, y desde la perspectiva tecnológica, se han realizado esfuerzos para contribuir con el propósito institucional, donde se incluyen: equipar con equipo de cómputo a las diferentes dependencias del INACIF, crear una infraestructura de red institucional y automatizar diferentes procesos mediante la implementación de una serie de herramientas de *software* que son de propósito específico.

1.1.2. Misión

Somos la Institución responsable de brindar servicios de investigación científica forense fundamentada en la ciencia y el arte, emitiendo dictámenes periciales útiles al sistema de justicia, mediante estudios medicolegales y análisis técnico-científicos, apegados a la objetividad y transparencia. (Instituto Nacional de Ciencias Forenses, 2020, p. 2)

1.1.3. Visión

Para el Instituto Nacional de Ciencias Forenses (2020) su visión es “ser una institución referente a nivel nacional e internacional, por su recurso humano competente, capacidad tecnológica, buenas prácticas forenses, calidad y transparencia en la gestión institucional y respeto a la dignidad humana” (p. 2).

1.2. Servicios que realiza

Según su demanda diaria así es el control de recepción de servicios, algunos para expedientes en legales en curso y otros por investigación común.

1.2.1. Clínica Forense

Efectúa pericias relacionadas con evaluaciones médicas a persona vivas. Dictamina sobre lesiones personales: determina mediante examen médico el daño que un agresor ocasiona a la integridad personal de un individuo (lesiones). Evalúa si una persona pudo haber sido víctima de una agresión sexual.

1.2.2. Odontología Forense

Determina lesiones personales en cavidad oral, dictamina sobre la edad cronológica e identifica a personas fallecidas mediante cotejo de su dentadura con la ficha dental.

1.2.3. Psiquiatría Forense

Determina en muchos casos la imputabilidad del sospechoso, además de evaluar su perfil psicológico y algunos trastornos emocionales.

1.2.4. Tanatología Forense

Realiza necropsias medicolegales para establecer la causa de la muerte y recolectar indicios que orienten al investigador, así como individualizar a la persona. Efectúa necropsias medicolegales a cadáveres exhumados por orden de autoridad competente.

1.2.5. Histopatología Forense

Realiza estudios de células y tejidos para determinar la presencia o desarrollo de procesos patológicos que pudieran haber incidido en casos cuyo contexto debe ser aclarado desde la perspectiva médico legal.

1.2.6. Antropología y Arqueología Forense

Realiza análisis e interpretación de restos óseos con fines de identificación, cuando fuera posible; restauración y reconstrucción cráneo facial. Realiza análisis arqueológicos de restos para determinar edad.

1.2.7. Psicología Forense

Psicología determina secuelas dejadas por agresión sufridas por la víctima o estado del individuo al agredir.

1.2.8. Laboratorio de Acústica Forense

En el Laboratorio de Acústica del INACIF se realizan peritajes de análisis de voz con el objeto de establecer si las muestras objeto de análisis son aptas o no, para un estudio comparativo (cotejo de voz), para concluir la correspondencia o exclusión entre las características de la voz, utilizando para ello, métodos y técnicas cualitativas y cuantitativas validados en el ámbito forense internacional; siendo así, una herramienta trascendental en la investigación criminal.

1.2.9. Laboratorio de Documentos, copia Forense

Es la encargada de realizar pericias a efecto de determinar alteraciones de documentos u cotejo de grafías y firmas. Puede determinar alteraciones en escrituras, protocolos, licencias, pasaporte, papel moneda entre otros muchos, sin incluir la capacidad con que se cuenta de determinar si algún texto fue o no escrito por la persona de la que se sospecha o si una firma fue o no elaborada por la persona a quien se le adjudica. Su aporte es de alta incidencia en casos de impacto.

1.2.10. Laboratorio de Balística Forense

Es la encargada de realizar peritajes propios de balística comparativa e identificativa, específicamente coteja los indicios ubicados en escena o en el

cuerpo de la víctima con elementos indubitados generados por el arma sospechosa. Puede llegar a determinar con certeza si fueron o no disparados por el artefacto, generando con ello aportes de mucha implicación en investigaciones criminales.

1.2.11. Laboratorio de Toxicología Forense

Encargada de realizar análisis sobre fluidos tomados de personas vivas o cadáveres, con el fin de determinar presencia de sustancias que pudieran causar daños o la muerte, normalmente la búsqueda de las sustancias enfoca drogas de abuso y alcohol.

1.2.12. Laboratorio de Lofoscopía Forense

Esta sección puede con certeza llegar a identificar plenamente a la persona que dejó huella en un objeto que pudiera ser el elemento de concatenación para la investigación de un hecho. Es además la responsable de cotejar las impresiones obtenidas de los dedos de personas fallecidas que no han sido identificadas, con ello de manera rápida y totalmente confiable se determina su identidad, al comparar con las bases de datos civiles, municipales o criminales del país.

1.2.13. Laboratorio Serología y Genética Forense

Laboratorio de altísimo impacto en la investigación, ya que realiza una serie de análisis bioquímicos para determinar en caso de agresiones sexuales o casos en que se da lucha entre agresor y víctima la presencia de fluidos además lleva a cabo análisis de ADN sobre fluidos identificados y en los cuales

existe elementos de comparación. La virtud de los fluidos al igual que la dactiloscopia es la enorme capacidad individualizarte de sus resultados.

1.2.14. Laboratorio Identificación de Vehículos

Los vehículos son uno de los aspectos que nutre el crimen organizado; la sección está en la capacidad de determinar alteraciones en los automotores, establecer con ello la individualización de vehículos y dar aportes contundentes para establecer si los mismos han sido alterados.

1.2.15. Laboratorio Fisicoquímica Forense

Esta sección maneja las trazas, -entiendo como trazas elementos que por la lucha víctima sospechoso generan transferencias-, su aporte puede llegar a ser altísimo siempre quedando sujeta a los aportes que en materia de elementos indubitados del ente investigador.

1.2.16. Laboratorio Sustancias Controladas

Las drogas ilícitas y los precursores son uno de los elementos claves a controlar para poder lograr la paz social. Desde este contexto esta sección genera aportes de alta valía al analizar los materiales cuyo modelo de tráfico es compatible con drogas como la cocaína, heroína, éxtasis entre otras muchas.

1.2.17. Laboratorio de Informática Forense

Es una disciplina auxiliar de la justicia moderna, que mediante las técnicas de adquisición, preservación, obtención y presentación de datos que han sido procesados y almacenados en medios electrónicos, como discos

duros, memorias USB, tarjetas de memoria, teléfonos inteligentes, entre otros, son aceptados dentro de un proceso legal.

1.3. Descripción de necesidades

El presente proyecto de EPS, surge a partir de tener varios sistemas de información basados en la web, con usuarios locales propios, llevando al problema de que una persona puede estar registrada en varias aplicaciones web, y por lo tanto tener varios usuarios diferentes, resulta ser un problema cuando ya se tienen varios sistemas de información basados en la web por institución, ya que al usuario final le resulta tedioso estar memorizando credenciales para cada sistema de la institución y a nivel de desarrollo, resulta complicado llevar un control de tantos usuarios.

Para presentar una solución al problema, se presentan 3 necesidades básicas las cuales son: 1. encontrar un *software* que administre el inicio de sesión inicio, en lugar de que las aplicaciones web lo manejen de manera interna, 2. establecer un sistema, en el cual nuevos sistemas de información basados en la web, puedan hacer uso del inicio de sesión único, 3. Integrar los sistemas de información basados en la web ya existentes del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses, en el sistema de inicio de sesión único.

1.4. Priorización de necesidades

Reconocer las necesidades básicas para llevar la realización del proyecto, se estableció el siguiente orden para llevar el desarrollo del proyecto de manera adecuada.

2. FASE TÉCNICO PROFESIONAL

2.1. Descripción del proyecto

Se reconoce como un sistema al conjunto relacionado de elementos entre sí que puede funcionar como un todo constantemente, por lo que este proyecto surge de la necesidad de tener un sistema de inicio de sesión único para todos los sistemas de información basados en la web que existen actualmente, y que existirán, en términos generales, lo que se necesita es establecer un sistema, que maneje las sesiones de los usuarios.

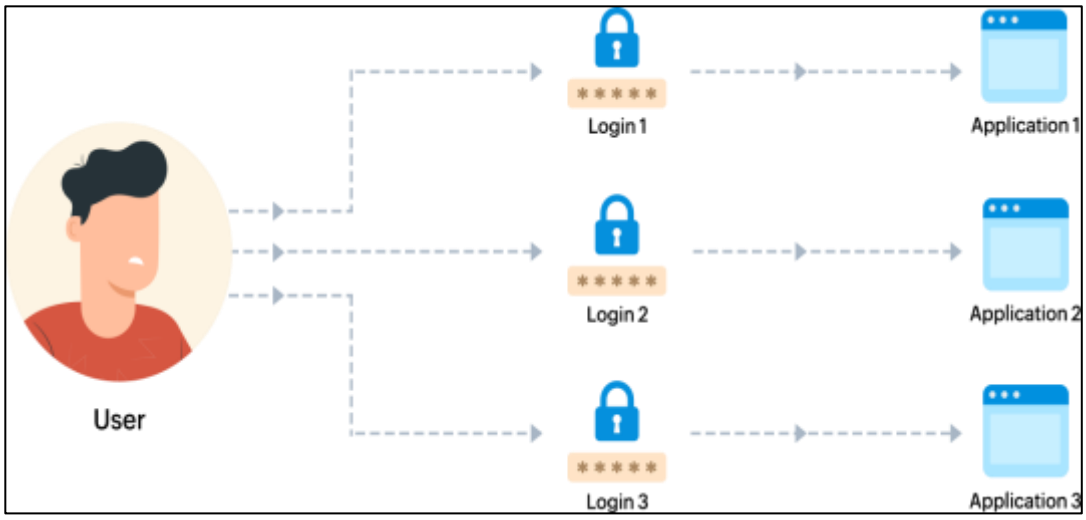
El problema principal al cual se le debe dar solución es que ya existen suficientes sistemas de información basados en la web y seguirán existiendo más, cada uno cuenta con usuarios locales propios de cada sistema de información basado en la web, por lo que una persona puede llegar a tener varios usuarios, uno en cada sistema de información basado en la web, lo cual, a nivel de desarrollo en la Unidad de Informática, se presenta como una descentralización de información y dificulta darle un seguimiento como tal.

La implementación de un sistema de inicio de sesión único facilitaría el acceso de los empleados del Instituto Nacional de Ciencias Forenses a múltiples portales web, ahorrando tiempo, reduciendo la carga de memorizar diferentes credenciales, mejorando la gestión de datos de usuario. El proyecto denominado con el nombre de ¨Sistema de inicio de sesión único para aplicaciones del departamento técnico científico del Instituto Nacional de Ciencias Forenses de Guatemala¨ lo que busca es establecer un sistema de inicio de sesión único, que este sistema sea viable para los nuevos sistemas de

información basados en la web en desarrollo y que se desarrollaran en un futuro, e integrar los sistemas de información basados en la web del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses de Guatemala, al sistema de inicio de sesión único.

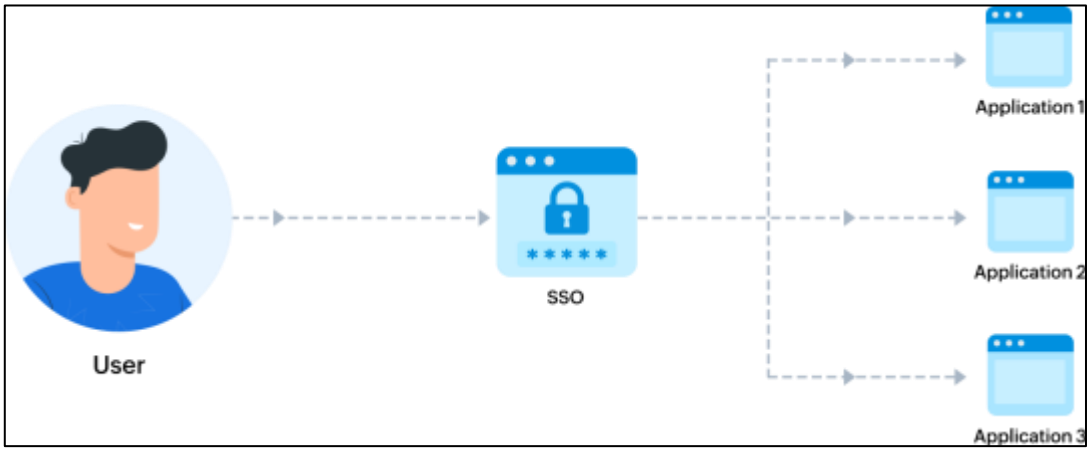
Actualmente, el flujo de datos, para iniciar sesión, en cada sistema de información basado en la web del Instituto Nacional de Ciencias Forenses de Guatemala, se encuentra como esta descrito en la figura 1., lo que se busca con el sistema de inicio de sesión único, es establecer un único flujo de inicio de sesión, para todos los sistemas de información basados en la web, como se demuestra en la figura 2.

Figura 1. **Flujo de datos para acceder a un sistema de información basado en la. web, sin sistema de inicio de sesión único**



Fuente: ManageEngine (2021). *Un usuario y diversos puntos de red*. Consultado el 14 de febrero de 2021. Recuperado de https://www.manageengine.com/products/self-service-password/what-is-single-sign-on-and-how-sso-works.html.

Figura 2. **Flujo de datos para acceder a todos los sistemas de información basados en la web, con sistema de inicio de sesión único**



Fuente: Manage Engine (2021). *Un usuario y diversos puntos de red.* Consultado el 14 de febrero de 2021. Recuperado de https://www.manageengine.com/products/self-service-password/what-is-single-sign-on-and-how-sso-works.html.

2.2. Justificación del proyecto

Se priorizan las necesidades del Instituto Nacional de Ciencias Forenses de Guatemala conforme a sus necesidades de implementar mejoras continuas informáticas en sus modelos internos de procesamiento de información.

2.2.1. Técnica

El Instituto Nacional de Ciencias Forenses de Guatemala, al ir creciendo en el área de desarrollo de *software* a un nivel exponencial, se ve en la necesidad de centralizar la información requerida para la autenticación y autorización en sus portales web. El proyecto unifica la autenticación de todas

las plataformas en un único sistema de autenticación y estandariza la integración de este servidor a futuros proyectos a crear dentro de la institución.

2.2.2. Social

Esta implementación tendrá un impacto dentro de los trabajadores, lo cual busca reducir la cantidad de usuarios y contraseñas que estos debían memorizar, ya que, al ser una institución con bastante alcance, estos llegan a tener una persona con varios usuarios para acceder a cada plataforma en las cuales estos tienen acceso, con un usuario y contraseña diferente.

2.3. Investigación preliminar para la solución del proyecto

Con base en las debilidades encontradas durante la investigación se presentan un conjunto de acciones necesarias para dar solución al proyecto.

2.3.1. Inicio de sesión único

También conocido como SSO (Single Sign-on), es un método de autenticación que permite a los usuarios a acceder a múltiples sistemas de información basados en la web con un procedimiento de inicio de sesión por medio de un único conjunto de credenciales, es decir un nombre de usuario y una contraseña.

2.3.2. ¿Por qué implementar un sistema de inicio de sesión único?

Por facilidad de uso y sencillez de gestión, para el usuario final, resulta más fácil, tener un único conjunto de credenciales para poder ingresar a cada

sistema de información basado en la web, y de esta forma, la Unidad de Informática del Instituto Nacional de Ciencias Forenses de Guatemala, podría llevar un mejor control de los usuarios, ya que se centralizaría la información de las credenciales de los usuarios, para la centralización de la información, se aprovechará que la institución actualmente, cuenta con un Active Dierctory, obteniendo la información de los usuarios por medio de este.

2.3.3. Desventajas de implementar un inicio de sesión único

La mayor desventaja de esta implementación es que si una tercera persona consiguiera un usuario y contraseña, podría tener acceso a todos los sistemas de información basados en la web, del que esas credenciales tengan alcance. Otra desventaja que considerar es la alta disponibilidad, ya que el Sistema de Inicio de Sesión Único no puede estar inactivo, porque esto podría provocar que los usuarios finales no puedan acceder a las aplicaciones.

2.3.4. *Software* de SSO

Es una solución de autenticación que se usan algunas empresas para proteger los accesos a sus aplicaciones, este *software* provee a los usuarios finales un portal, en el que se inicia sesión una vez para acceder a las aplicaciones de la empresa. El *software* de SSO funciona compartiendo sesiones de autenticaciones entre un proveedor de identidad, que administra identidades digitales y aplicaciones, el proveedor de identidad requiere que el usuario inicie sesión y se autentique, seguido el proveedor de identidad comparte la sesión con el resto de las aplicaciones pasando *tokens* firmados digitalmente para que la aplicación receptora verifique que proviene de un proveedor confiable, y pueda otorgar acceso a la aplicación.

Para el desarrollo del proyecto de EPS, se requiere encontrar un *software* que brinde el servicio de inicio de sesión único, ya que en la actualidad existen varios *softwares* que bridan este servicio, que son de código abierto, la cuestión es cuál de los *software* de SSO de código abierto, se acoplan mejor a la necesidad del Instituto Nacional de Ciencias Forenses de Guatemala de tener un único portal de inicio de sesión, teniendo en cuenta que este *software* se tiene que aplicar con las aplicaciones ya existentes y que estas aplicaciones a nivel de *software* están un poco rezagadas.

2.3.5. Características de un *software* de SSO

Los *softwares* de SSO, comparten características en comunes entre sí, que son esenciales para una implementación correcta de este servicio.

- Portal de usuario: es la interfaz que permite a los usuarios configurar el *software* de SSO.

- Métodos MFA: autenticación de múltiples factores (MFA); son múltiples tecnologías para autenticar a un usuario, como podría ser autenticación basada en *tokens*, autenticación biométrica o códigos de acceso de un solo uso.

- Directorio de integración: son las distintas maneras de proveer usuarios al *software* de SSO como la integración con directorios basados en LDAP.

- Gestión de roles: es la función que permite administrar la autorización de los usuarios finales en las aplicaciones, por medio de la asignación de permisos.

- Funciones de auditorías: proporcionan a los administradores registros para monitorear el acceso de los usuarios.

2.3.6. *Softwares* de SSO candidatos a implementar

Se realizó una previa investigación de los *softwares* existentes y algunas de sus características principales, para analizar cuál es el que se acopla mejor a la necesidad el Instituto Nacional de Ciencias Forenses.

Tabla I. ***Softwares* SSO candidatos**

Software	¿Es de pago?	Descripción
Keycloak	No	Es un *software* de código abierto, proporciona gestión de identidad y una interfaz de inicio de sesión único, proporciona dos componentes principales que involucran servidor y adaptador de aplicación. Brinda bastante documentación, está respaldado por RedHat.
One Login	Si	Es un *software* de gestión de identidad, basado en la nube que diseña y vende esta solución. Su gestión de identidad y acceso es rápida.
Auth0	SI	*Software* con arquitectura robusta, plataforma que gestiona la autenticación y autorización, y se integra con todo tipo de dispositivos digitales.
Systematic Siteminder	Si	Proporciona una plataforma que administra el inicio de sesión único, es fácil de usar, brinda acceso seguro, permite conectar todas las aplicaciones en la nube.

Fuente: elaboración propia, realizado con Microsoft Word.

2.3.7. Sistemas de información basados en la web por integrar en el sistema de inicio de sesión único

El Instituto Nacional de Ciencias Forenses de Guatemala actualmente ya cuenta con distintos sistemas de información basados en la web, que se necesitan integrar al Sistema de Inicio de Sesión Único, este requerimiento para el desarrollo del proyecto de EPS es de alta prioridad. A continuación, se establecerán los sistemas de información basados en la web, que se van a integrar al Sistema de Inicio de Sesión Único.

Tabla II. **Sistemas de información basados en la web del Instituto Nacional de Ciencias Forenses de Guatemala**

Nombre de la plataforma	Nombre abreviado	Tecnología en la cual se encuentra desarrollada	Alcance
Sistema de Gestión Nacional Forense	SINAF	Java Web	Todos los empleados del Departamento Técnico Científico del Instituto Nacional de Ciencias Forenses de Guatemala.
Sistema de Huellas Dactilares	SIHUDA	Java Web	Empleados del área de Lofoscopia Forense y Unidad de Medicina Forense del Instituto Nacional de Ciencias Forenses de Guatemala.
Sistema de Planificación para Seguimiento del Plan Estratégico Institucional	PEI	Java Web	Todos los empleados del Instituto Nacional de Ciencias Forenses de Guatemala.

Continuación de la tabla II.

Nombre de la plataforma	Nombre abreviado	Tecnología en la cual se encuentra desarrollada	Alcance
Sistema de Adhesión de Certificado de Firma Electrónica Personal e Institucional para documentos del INACIF	DOCSIGN	Java Web	Todos los empleados del Instituto Nacional de Ciencias Forenses de Guatemala.

Fuente: elaboración propia, realizado con Microsoft Word.

2.4. Presentación de la solución del proyecto

Posteriormente a evaluar los puntos críticos que destacan en la investigación se realiza la presentación de la solución.

2.4.1. Detalles técnicos de la solución

Un inicio de sesión único para múltiples plataformas es un proceso que habilita a un usuario predeterminado acceder varios sistemas con una sola instancia de identificación, es de gran utilidad cuando existen varias plataformas y se busca centralizar la información de los usuarios. Se creará un canal único de autenticación de usuarios por medio de un sistema de *tokens*. A continuación, se muestra una breve descripción técnica de las herramientas que se utilizaron para la elaboración del proyecto.

Tabla III. **Herramientas de solución**

Herramienta	Descripción
OAuth2.0	Es un protocolo de autorización, que permite a las aplicaciones obtener acceso, a las cuentas de usuario de determinados servicios, delega la autenticación de usuario al servicio que gestiona las cuentas.
Java Web	Lenguaje de programación orientado a objetos, es rápido, seguro y confiable, utilizado de manera recurrente para desarrollar *backend* en aplicaciones web.
Keycloak	*Software* de código abierto que permite el inicio de sesión único con *Identity Management* y *Access Management* para aplicaciones y servicios modernos. Se encuentra bajo licencia de Apache y respaldado por *RedHat.*
Docke*r*	Tecnología de contenedorización de código abierto, para crear y contener aplicaciones, permite empaquetar un programa con todo lo necesario para funcionar, se empleará para desplegar el *software* de *Keycloak*.
Docker Compose	*Compose* es una herramienta para definir y ejecutar aplicaciones *Docker* de varios contenedores. Se usa con *Docker Compose* un archivo YAML para configurar los servicios de su aplicación.
*O*penID Connect	Protocolo de autenticación, es una capa de identidad simple sobre el protocolo *OAuth* 2.0. Permite a los clientes verificar la identidad del usuario final basándose en la autenticación realizada por un servidor de autorización, así como obtener información de perfil básica sobre el usuario final de una manera interoperable y similar a REST.
Active Directory	Es un servicio de directorio, permite a los administradores administrar los permisos y el acceso a los recursos de la red, almacena datos como objetos; un objeto es un elemento único, como un usuario.
Maven	Es una herramienta de gestión de proyectos de *software* principalmente para proyectos *Java*, basado en el concepto de un modelo de objetos de proyecto (POM).
Apache	Es un *software* web gratuito y de código abierto, en el cual se ejecutan alrededor del 46 % de los sitios web del mundo.

Fuente: elaboración propia, realizado con Microsoft Word.

2.4.2. Elección del *software* de SSO

El *software* de SSO que se eligió fue *Keycloak*, una de las razones que llevo a dicha elección, es que *Keycloak* es un *software* de código abierto, está respaldado por *Redhat* que es conocido por sus aspectos de seguridad, tiene suficiente documentación para diversas tecnologías, es compatible con las tecnologías con las que el Instituto Nacional Ciencias Forenses de Guatemala quiere trabajar en la actualidad, y se puede integrar con las tecnologías de desarrollo de los sistemas de información basados en la web de *Java* que ya existen dentro de la institución.

Características esenciales que permiten que *Keycloak* sea un *software* viable en el desarrollo del proyecto de EPS.

Tabla IV. **Características *Keycloak***

Característica	Descripción
Inicio de sesión único	Los usuarios finales se autentican con *Keycloak*, en lugar de que se autentiquen en cada uno de los sistemas de información basados en la web de forma independiente, *Keycloak* provee una interfaz de *login*, solo necesitan iniciar sesión una vez para poder ingresar al resto de sistemas de información basados en la *web*.
Federación de usuarios	Permite proveer usuarios al *software* contactándose a servidores de LDAP o Active Directory existentes.
Consola de administración	Cuenta con una consola que permite gestionar de manera centralizada la configuración de *Keycloak*.
Protocolos estándar	Se basa en protocolos estándar y brinda soporte para *OpenID Connect*, *OAuth2.*0 y *SAML.*
Servicios de autorización	*Keycloak* proporciona servicio de autorización, permite administrar permisos de los sistemas de información basados en la web desde la consola de administración.

Fuente: elaboración propia, realizado con Microsoft Word.

2.4.2.1. Flujo de autenticación de *Keycloak*

El flujo de autenticación se basa en que el usuario final ingresa a un sistema de información basado en la web del Instituto Nacional de Ciencias Forenses de Guatemala, seguido *Keycloak* lo redirige a la login de *Keycloak* para que el usuario final se autentique en *Keycloak* y este pueda validar las credenciales, si son correctas permite el ingreso a los sistemas de información basados en la web del instituto registrados en *Keycloak*, al momento de que *Keycloak* permita el ingreso de los usuarios finales a los portales *webs*, este está proveyendo un *token* con estándar de JWT, que brinda información a los portales web, para que este pueda obtener la información necesaria para seguir con el flujo correcto de su funcionamiento.

2.4.2.2. Conceptos generales de *Keycloak*

Para la explicación del desarrollo del proyecto de EPS, se necesita aclarar dos conceptos básicos de *Keycloak*, de los cuales se harán mención en la explicación de la solución del proyecto de EPS.

Tabla V. **Conceptos *Keycloak***

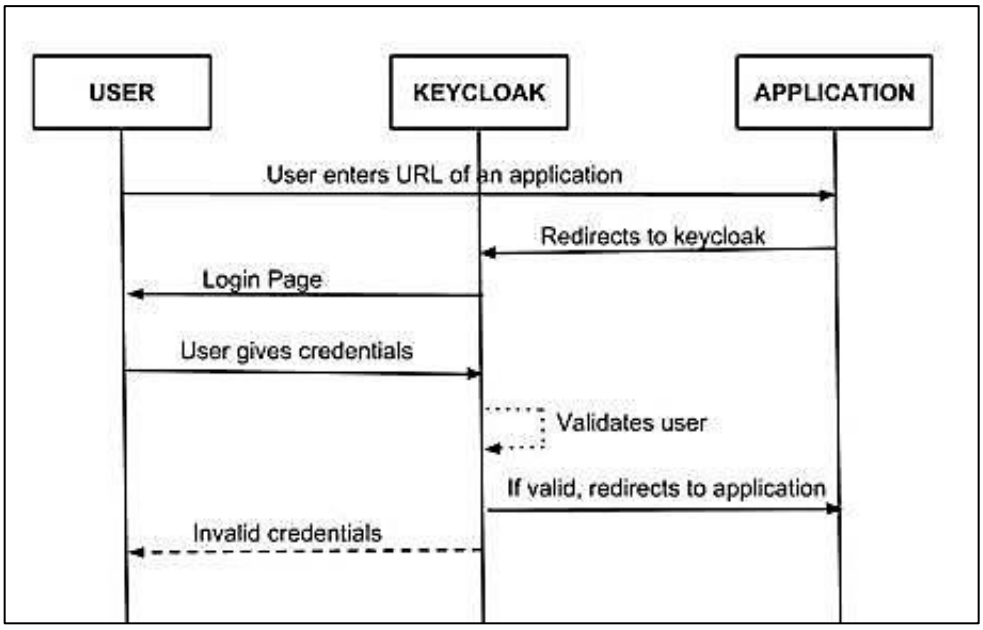
Características	Descripción
Reinos	Administra un conjunto de usuarios, credenciales roles y grupos. Un usuario inicia sesión en un reino, y los reinos se encuentran aislados unos de otros, así solo autentican y administran los usuarios que controlan.
Clientes	Son las entidades que pueden solicitar a *Keycloak* autenticar a un usuario. Para aplicación del desarrollo del proyecto de EPS, serían los sistemas de información basados en la web ya existentes del Instituto Nacional de Ciencias Forenses de Guatemala.

Fuente: elaboración propia, realizado con Microsoft Word.

2.4.2.3. Protocolo Open-Id connect

Se estableció que se van a integrar cuatro portales webs, ya existentes a Keycloa*k*, en estos portales se utiliza el protocolo de autenticación Open-id connect, esto permite que al ser consumido el inicio de sesión único en Keycloak, este proveerá de tokens, en formato JWT a los portales integrados, durante la definición del proyecto de EPS, se estableció que hay 2 elementos claves que deben ir contenidos dentro de este token, los cuales son CUI del empleado y el número de identificación propio de la institución.

Figura 3. **Flujo de datos para acceder a todos los sistemas de información basados en la web, con sistema de inicio de sesión único**

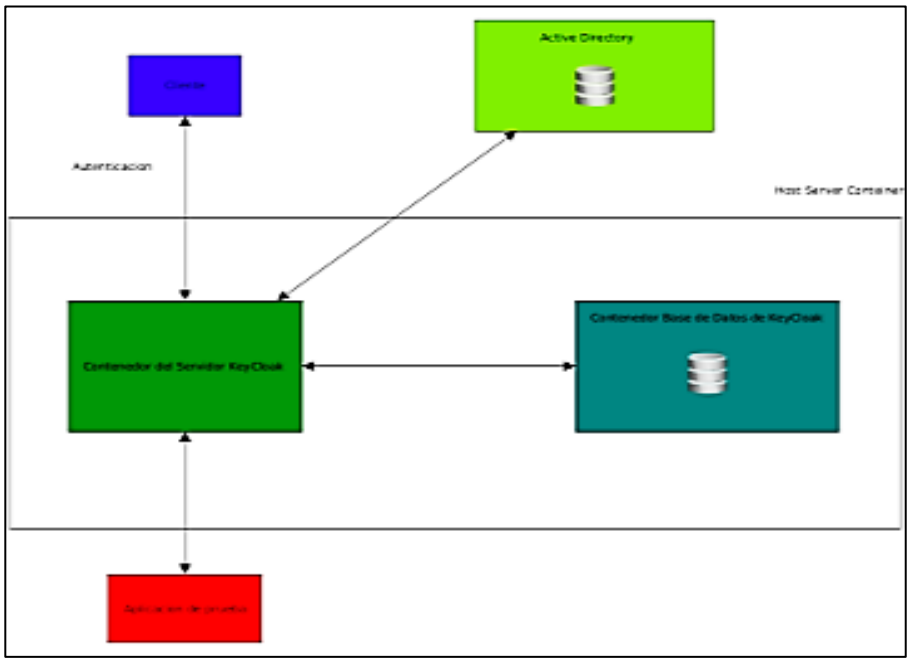


Fuente: Comakeit (2021). *El manejo ideal de los flujos de datos.* Consultado el 14 de febrero de 2021. Recuperado de https://www.comakeit.com/blog/quick-guide-using-*Keycloak*-identity-access-management/.

2.4.3. Arquitectura del Sistema de Inicio de Sesión Único

Para implementar un Sistema de Inicio de Sesión Único, se va *dockerizar* el servicio de Keycloak este provee el servicio de inicio de sesión único junto con una base de datos, la cual va acoplada con Keycloak para almacenar la información, el despliegue se realizará por medio de la herramienta de Docker Compose, el *software* de Keycloak se conectará al Active Directory para federar y proveer usuarios a Keycloak, los sistemas de información basados en la web consumirán el servicio de autenticación que proveen Keycloak, una vez los usuarios se autentiquen en Keycloak podrán acceder a los portales webs que estan registrados en los reinos de Keycloak. Una ventaja de Keycloak es que sus servicios de autenticación pueden ser consumidos por medio de REST API.

Figura 4. **Escenario de la arquitectura del Sistema de Inicio de Sesión Único**

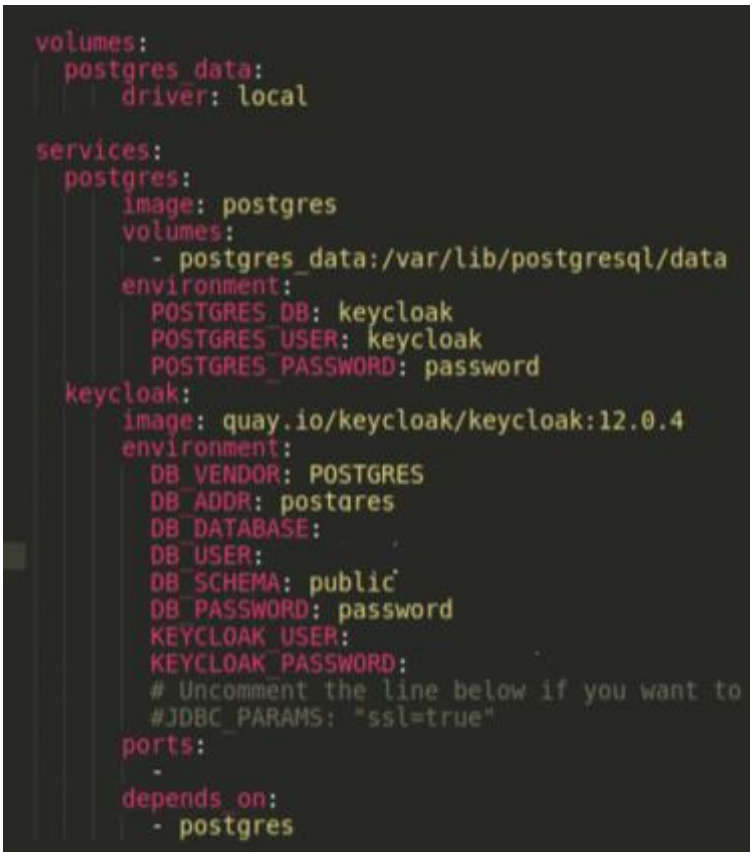


Fuente: elaboración propia, realizado con Microsoft Visio.

2.4.4. Implementación y configuración de *Keycloak*

A continuación, se describirán con imágenes paso a paso, la instalación y configuración de *Keycloak* por medio de *Docker* y *Docker Compose*. En la figura 5 se muestra la definición del archivo. yml para instalar *Keycloak*.

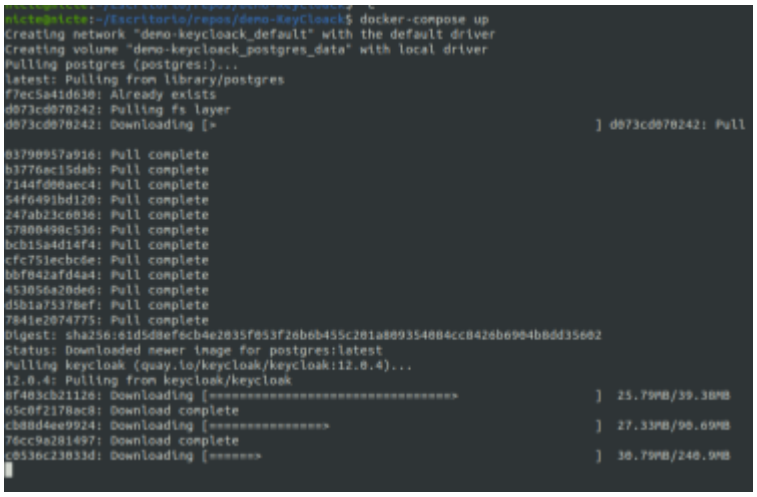
Figura 5. **Archivo. yml que instala *Keycloak***



Fuente: elaboración propia, realizado con *Keycloak*.

Instalando Keycloak por medio del servicio de contenedores, utilizando el comando de *docker-compose up*.

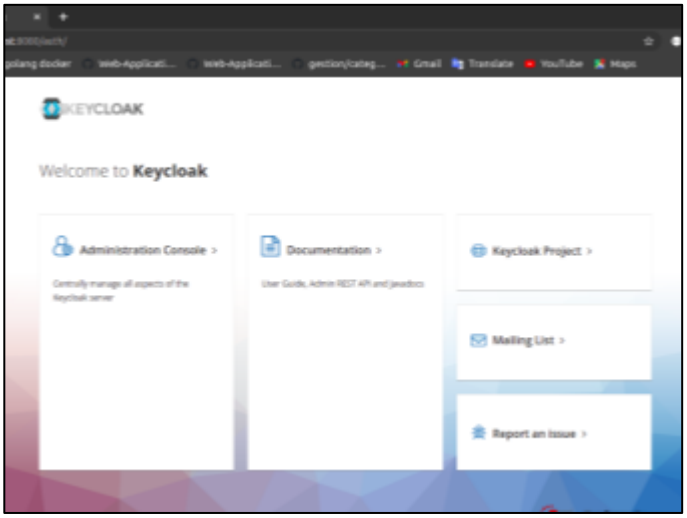
Figura 6. **Instalación de Keycloak**



Fuente: elaboración propia, realizado con *Keycloak*.

Accediendo a la interfaz de Keycloak:

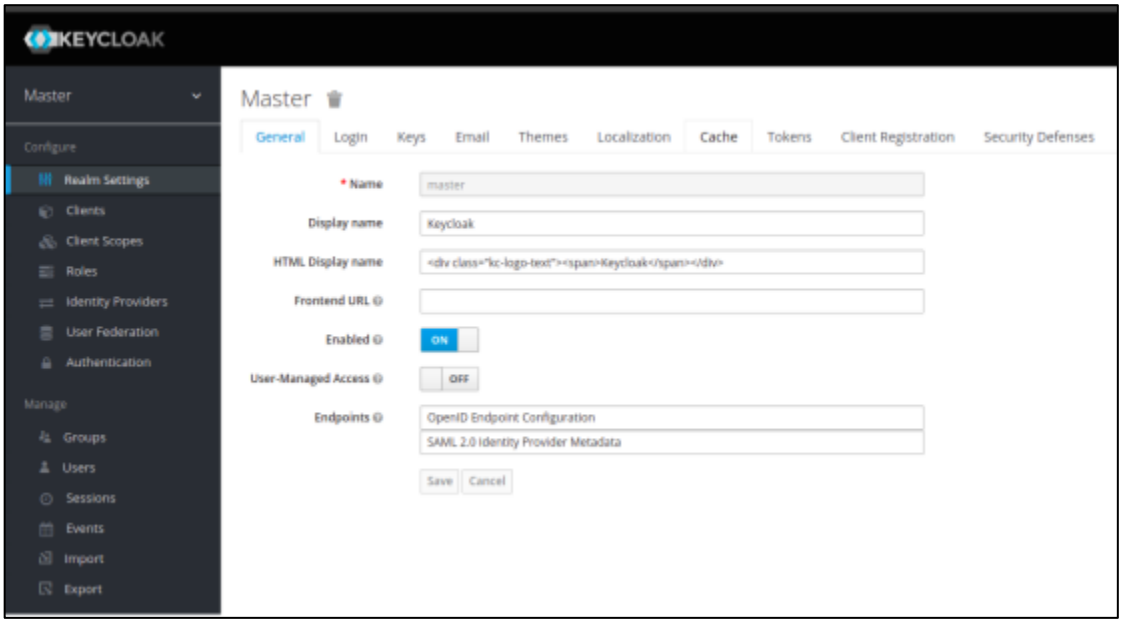
Figura 7. **Instalación de Keycloak**



Fuente: elaboración propia, realizado con *Keycloak*.

Accediendo a la consola de administrador de Keycloak.

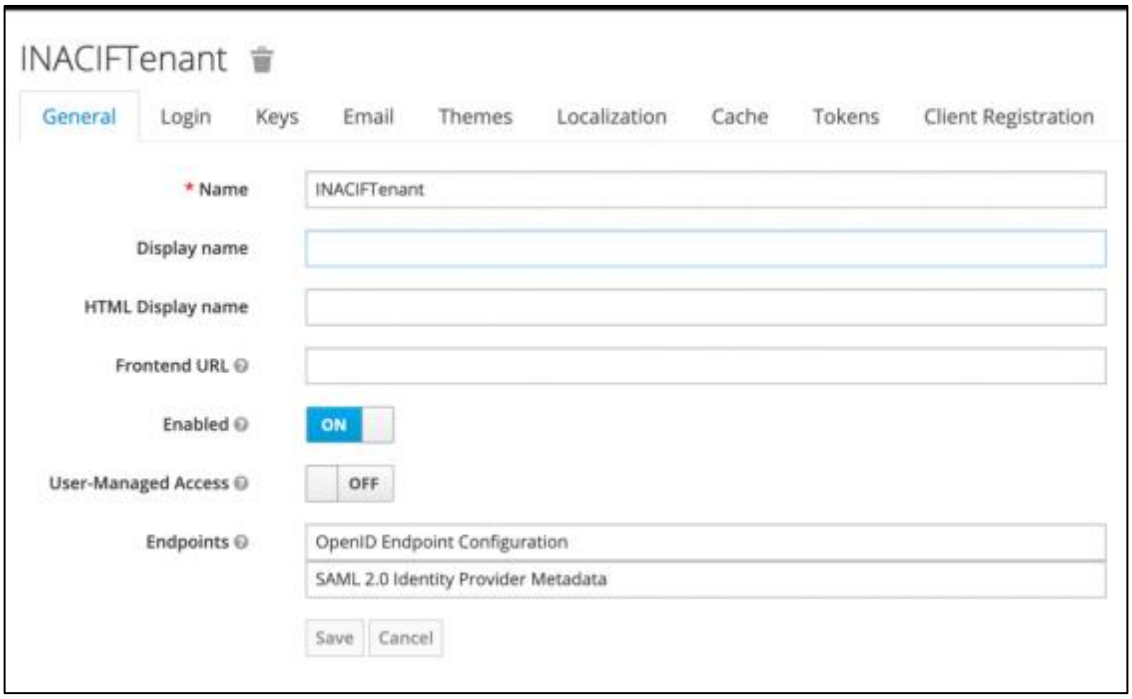
Figura 8. **Consola de administrador de Keycloak**



Fuente: elaboración propia, realizado con *Keycloak*.

Se creó un reino en la que se registrarán las aplicaciones webs del Instituto Nacional de Ciencias Forenses de Guatemala.

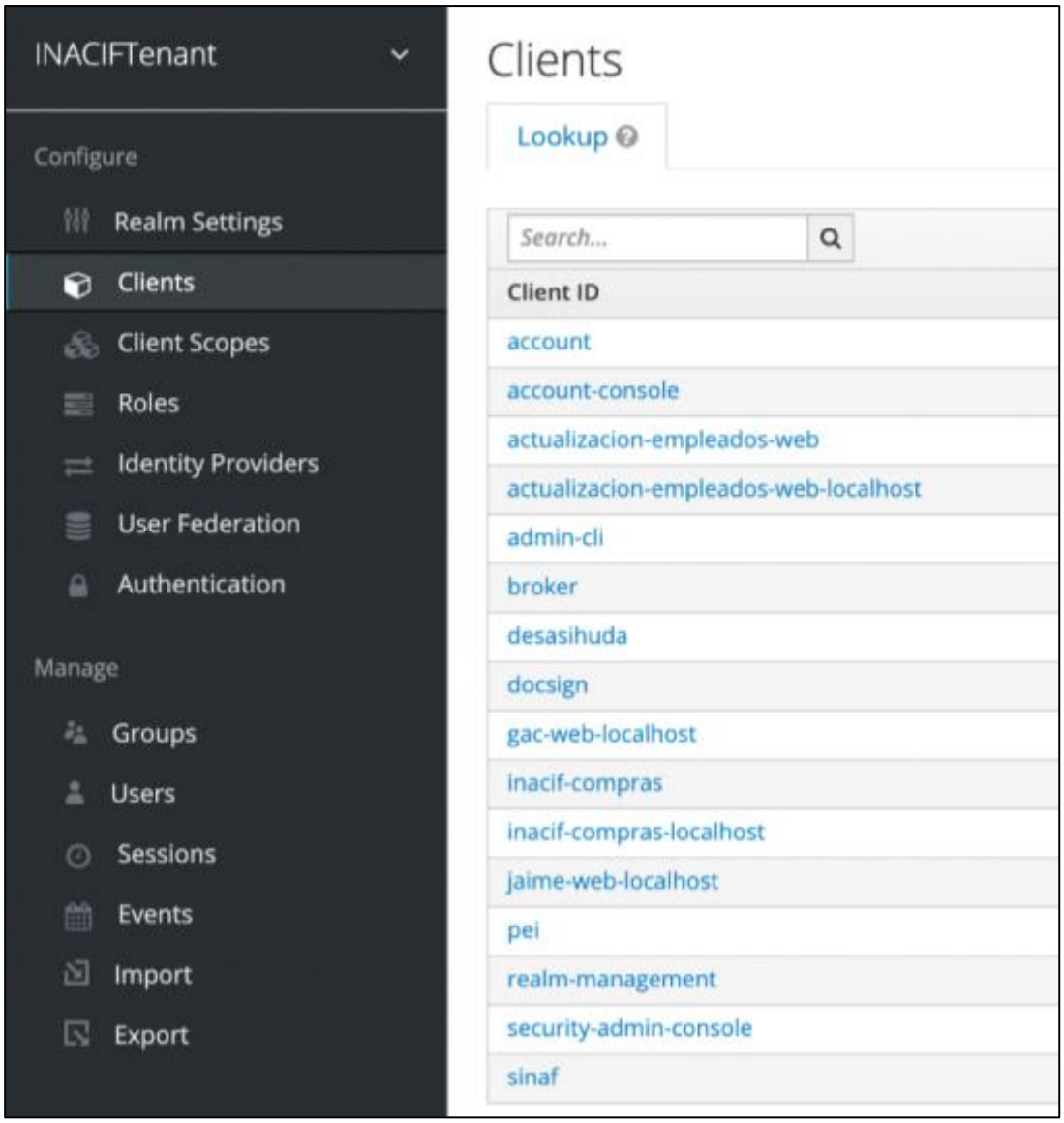
Figura 9. **Reino INACIFTenat en el que se registraron los sistemas de información basados en la web**



Fuente: elaboración propia. Realizado con *Keycloak*.

Se registraron como clientes los sistemas de información basados en la web, en el reino de INACIFTenat:

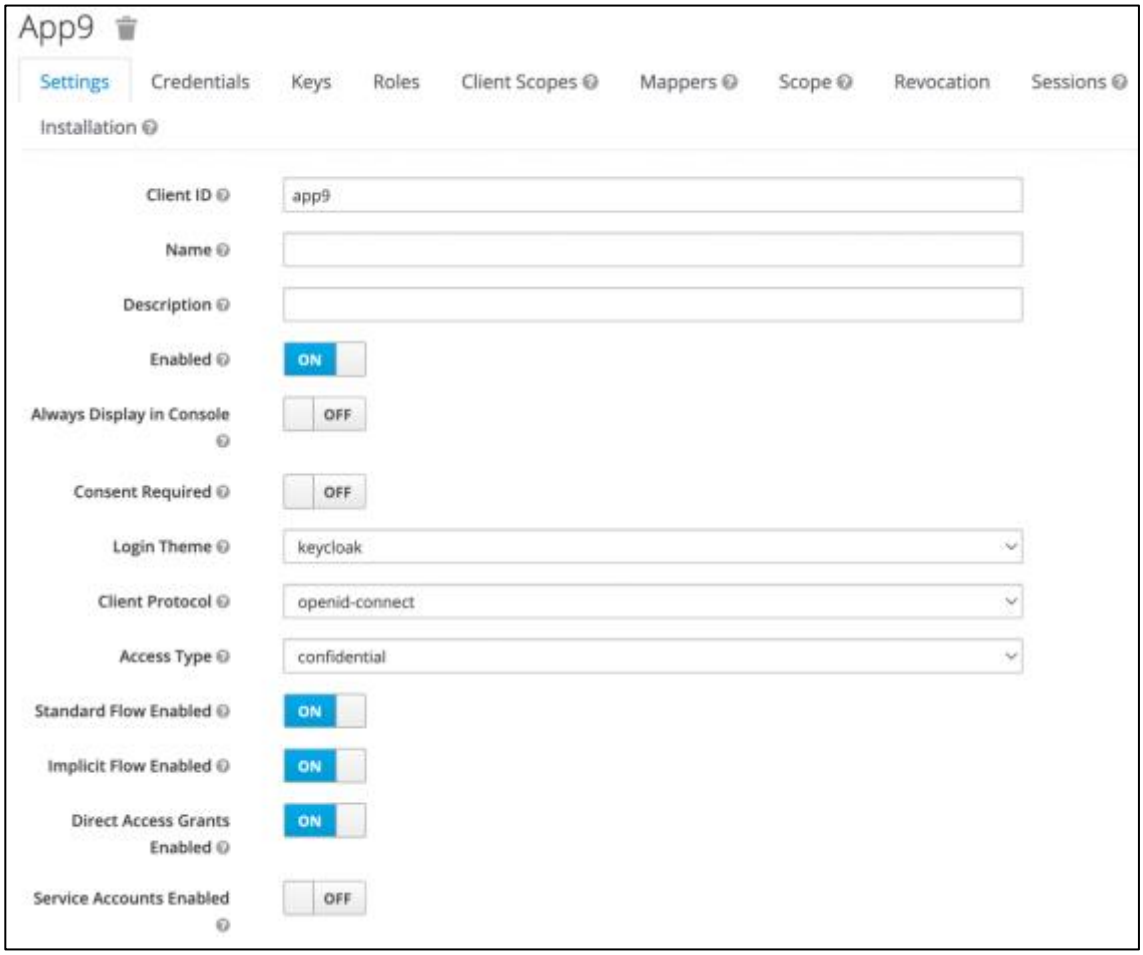
Figura 10. **Sistemas de información basados en la web registrados en *Keycloak***



Fuente: elaboración propia, realizado con Keycloak.

Se registran los 4 clientes en un reino de Keycloa*k*, en la figura 11 y figura 12, se muestra la configuración genérica de un cliente registrado en un cliente de Keycloak.

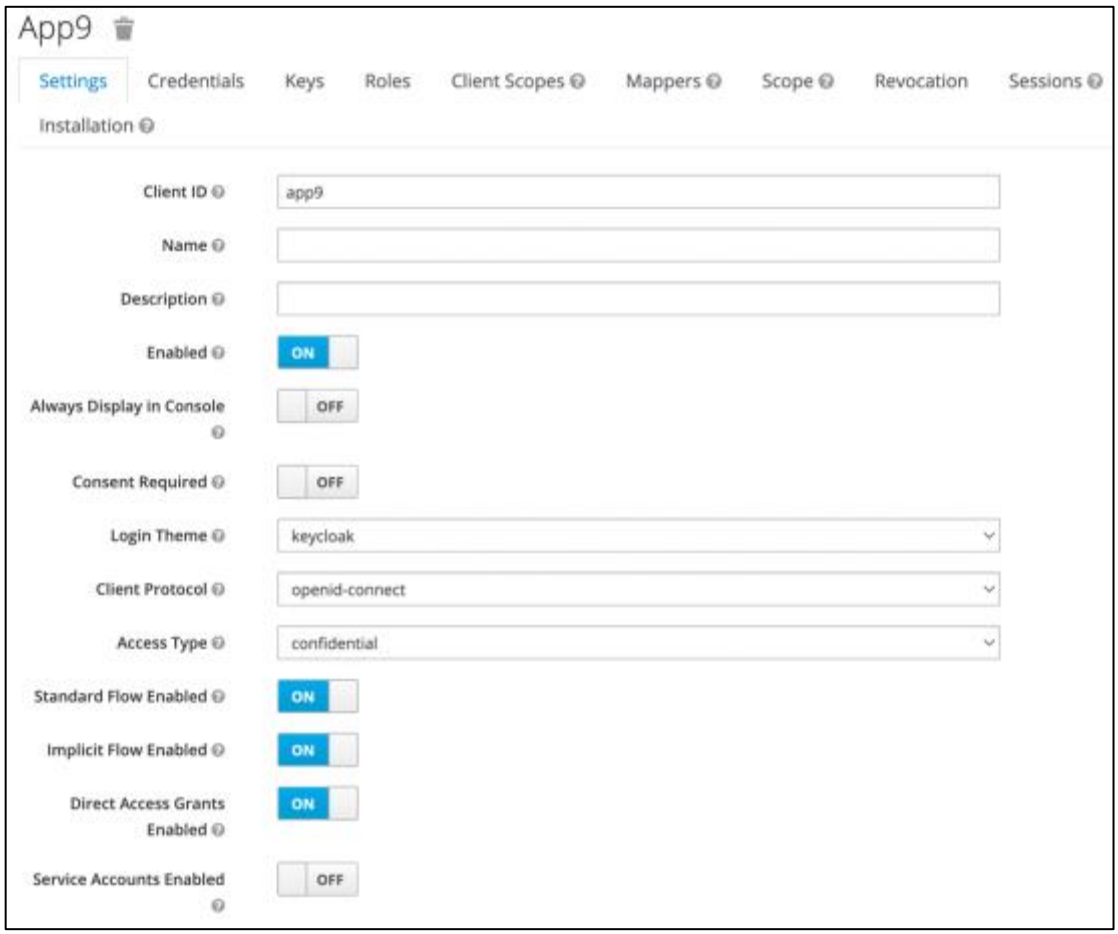
Figura 11. **Configuración cliente en Keycloak**



Fuente: elaboración propia, elaborado con *Keycloak*.

Es importante que los usuarios realicen dichas configuraciones para evitar duplicidad de usuario, retrasos en los accesos a la red u otros problemas asociados a la configuración general de los clientes.

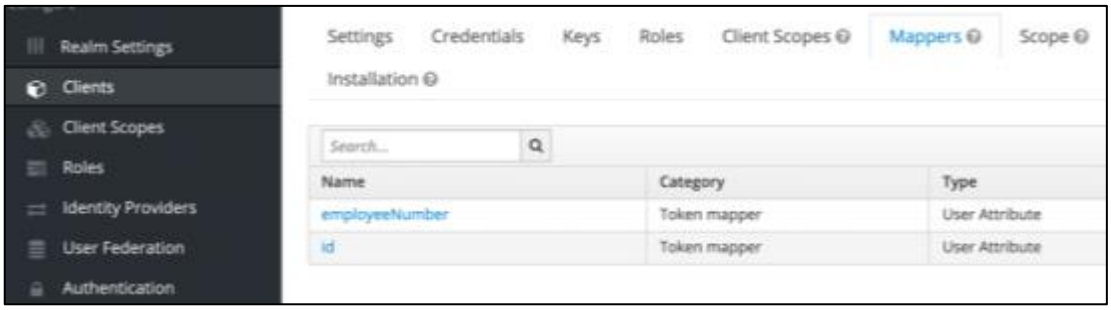
Figura 12. **Configuración de rutas en un cliente de Keycloak**



Fuente: elaboración propia, realizado con Keycloak.

En todos los clientes registrados en Keycloak los cuales son PEI, SIHUDA, DOCSIGN y SINAF, se registraron dos atributos que sirven para proveer información específica al momento que los portales webs, consuman el servicio de autenticación de Keycloak. Esto se realizó por medio del módulo de *mappers.*

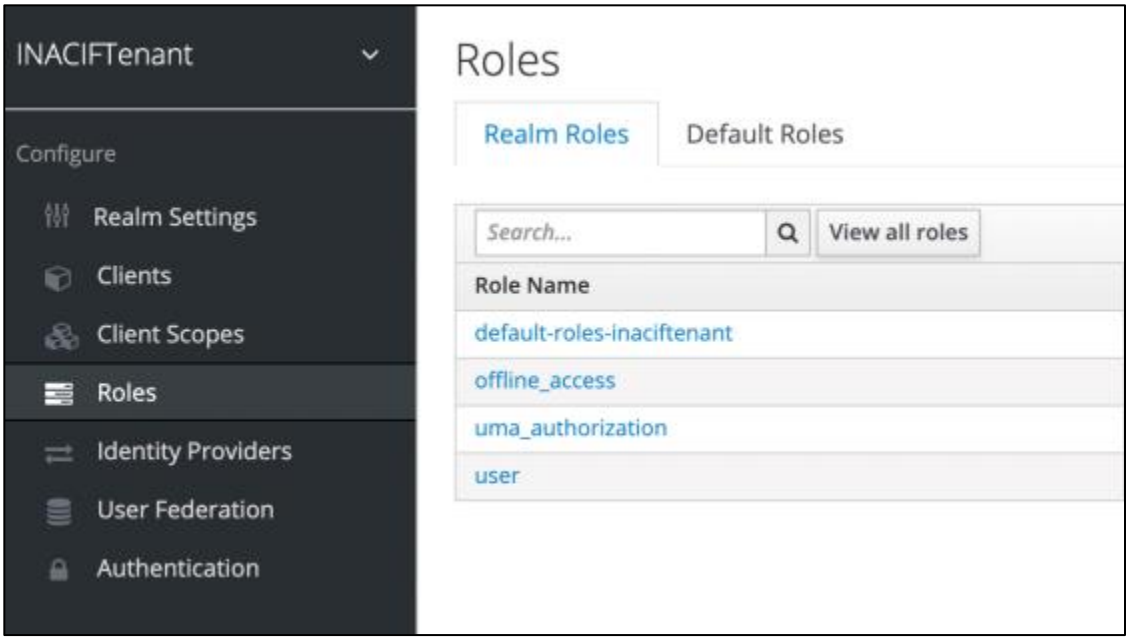
Figura 13. **Mappers *Keycloak***



Fuente: elaboración propia, realizado con *Keycloak*.

Se creó un rol, con el nombre de *user*, para asignarlo a los usuarios, y que los usuarios con ese rol puedan ingresar a los portales webs:

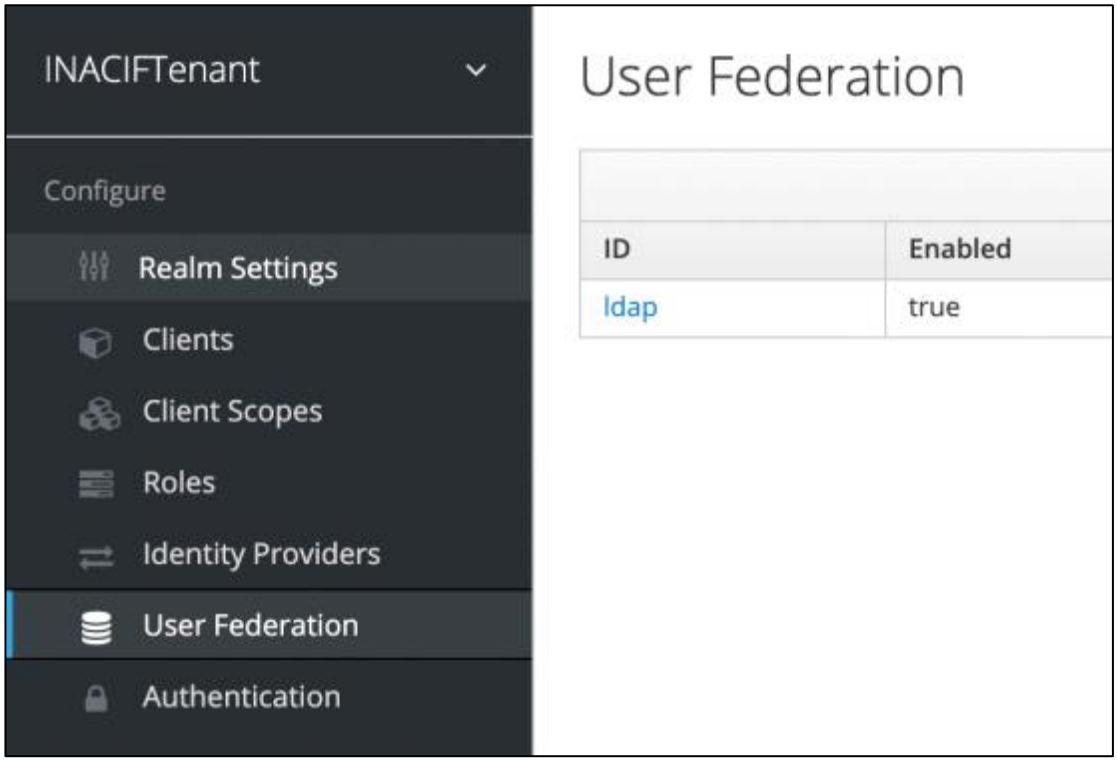
Figura 14. **Listado de roles registrados en el reino de INACIFTenat**



Fuente: elaboración propia, realizado con *Keycloak*.

Keycloa*k* permite proveer de usuarios integrando un Active Directory, por lo que se configuró un módulo de Keycloak, para poder agregar los usuarios del Active Directory del Instituto Nacional de Ciencias Forenses de Guatemala al reino de InacifTenat.

Figura 15. **User Federation**



Fuente: elaboración propia, realizado con *Keycloak*.

Figura 16. **Usuarios registrados en Keycloak a través del módulo de *user federation***

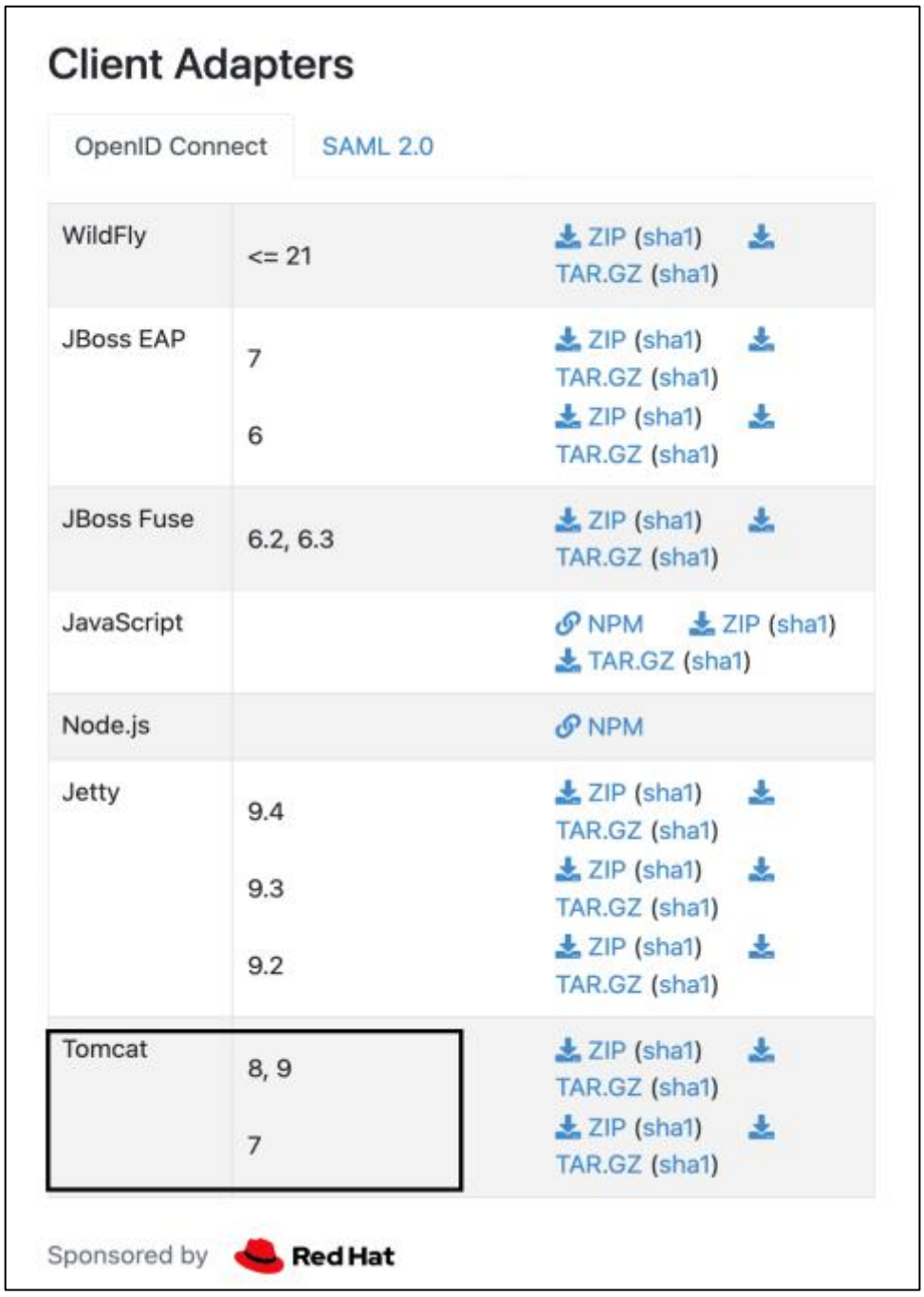
Fuente: elaboración propia, realizado con Keycloak.

2.4.5. Integrando Keycloak en el servidor *Apache Tomcat*

Los cuatro portales webs ya existentes en el Instituto Nacional de Ciencias Forenses de Guatemala, están desarrollados sobre el lenguaje de *Java* 8 y se encuentran publicados en un servidor de *Apache Tomc*at versión 7, se realizaron las configuraciones necesarias dentro del servidor, para poder consumir el servicio de autenticación de Keycloak.

Se descargan las librerías de Client Adapters, exactamente la versión 15.0.2, desde la página oficial de Keycloak, para *Tomcat* 7.

Figura 17. **Listado de librerías *Client Adapters* de Keycloak**



Client Adapters

OpenID Connect | SAML 2.0

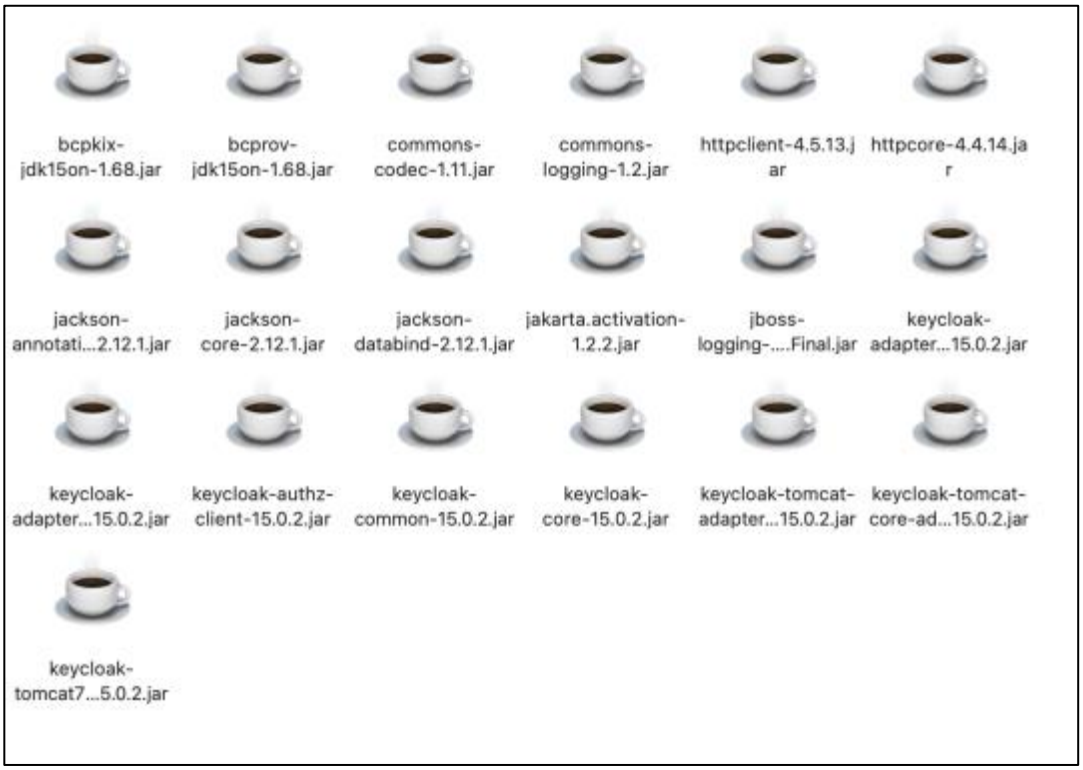
WildFly	<= 21	ZIP (sha1) TAR.GZ (sha1)
JBoss EAP	7	ZIP (sha1) TAR.GZ (sha1)
	6	ZIP (sha1) TAR.GZ (sha1)
JBoss Fuse	6.2, 6.3	ZIP (sha1) TAR.GZ (sha1)
JavaScript		NPM ZIP (sha1) TAR.GZ (sha1)
Node.js		NPM
Jetty	9.4	ZIP (sha1) TAR.GZ (sha1)
	9.3	ZIP (sha1) TAR.GZ (sha1)
	9.2	ZIP (sha1) TAR.GZ (sha1)
Tomcat	8, 9	ZIP (sha1) TAR.GZ (sha1)
	7	ZIP (sha1) TAR.GZ (sha1)

Sponsored by Red Hat

Fuente: elaboración propia, realizado con *Keycloak*.

Esto descarga una carpeta comprimida que contiene varias librerías .jar, las cuales hay que importarlas al servidor de *Apache Tomcat*, este servidor es en donde se levantan los portales web.

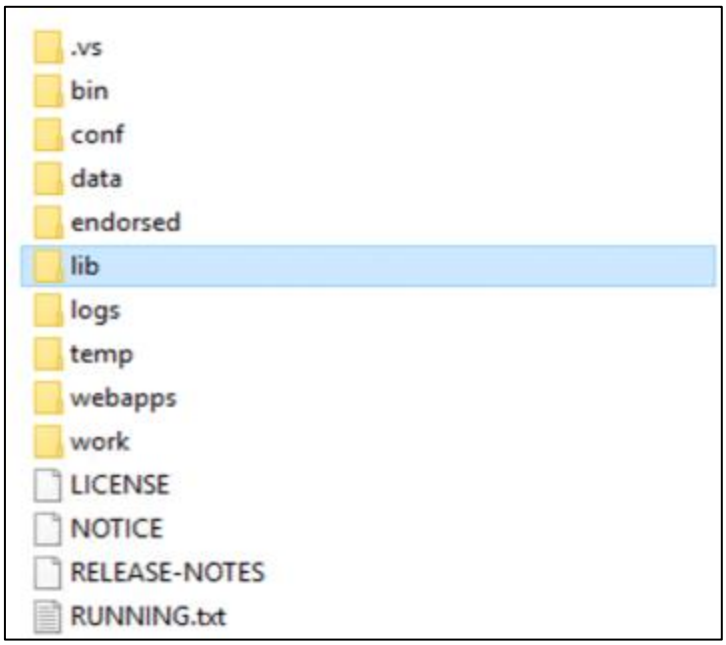
Figura 18. **Librerías de Keycloak importadas al servidor de Apache Tomcat**



Fuente: elaboración propia, realizado con Keycloak.

Se importan las librerías en la carpeta libs, del servidor de Apache Tomcat.

Figura 19. **Carpetas del servidor de Apache Tomcat**



Fuente: elaboración propia, realizado con Microsoft Visio.

Se empieza la modificación del código de los portales a nivel de desarrollo. Dentro de la solución de los portales del Instituto Nacional de Ciencias Forenses, desarrollados en Java se encuentra un archivo con el nombre de context.xml, este archivo se modifica como se muestra en la figura 18.

Figura 20. **Context.xml**

```
<?xml version="1.0" encoding="UTF-8"?>
<Context antiJARLocking="true" path="[redacted]">
    <Valve className="org.keycloak.adapters.tomcat.KeycloakAuthenticatorValve"/>
</Context>
```

Fuente: elaboración propia, realizado con Neatbeans 8.2.

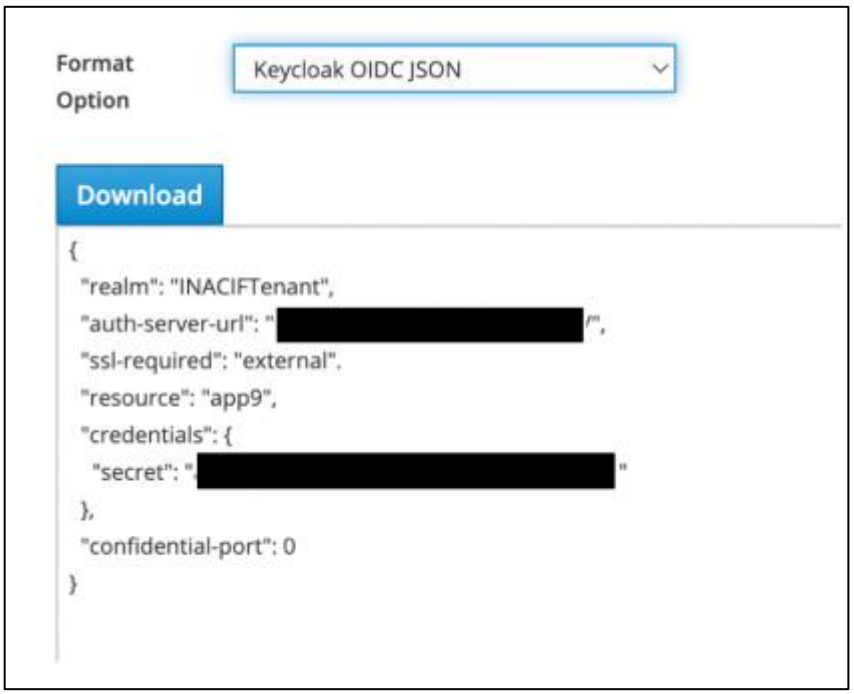
Se modifica el archivo web.xml, agregando la información que se indica en la Figura 19, como se puede observar se agrega el error de *user*, que fue agregado en la configuración de Keycloak.

Figura 21. **Web.xml**

Fuente: elaboración propia, realizado con Neatbeans 8.2.

En todos los portales webs en los que se van a integrar con Keycloak, se crea un archivo ‘Keycloak.json’, dentro de la carpeta ‘WEB-INF’, este archivo contiene la información, que brinda el propio software de Keycloak, dentro cada cliente registrado se cuenta con una pestaña con el nombre de *installation*, el cual permite obtener la información que se va a colocar dentro del archivo *Keycloak.json* creado, o bien se puede descargar el archivo directamente desde el *software* de Keycloak.

Figura 22. **Keycloak.json**



Fuente: elaboración propia, realizado con *Keycloak*.

2.4.6. Librerías instaladas en los portales web de la institución

Se descargaron 2 librerías que son oficiales de Keycloak y una que es oficial de Google, estas se importaron de manera individual en cada uno de los portales desarrollados en *Java* por medio del gestor de paquetes de Maven, el cual se gestiona por medio de un archivo que se llama pom.xml, el cual ya existe. Las versiones de las librerías instaladas son específicas, esto se debe a que los portales web se encuentran desarrollados sobre *Java* 8, y si se utiliza alguna librería que esté compilada sobre una versión de *Java* más reciente, podría de dar error al momento de compilar todo el código.

Tabla VI. **Librerías DOCSIGN**

Nombre	Versión	Proveedor
Keycloak-core	4.1.0 Final	org.Keycloak
Keycloak-core-adapter	4.8.0 Final	org.Keycloak
Gson	2.8.5	com.google.code.gson

Fuente: elaboración propia, realizado con Microsoft Word.

Tabla VII. ***Librerías PEI***

Nombre	*Versión*	*Proveedor*
Keycloak-core	4.1.0 Final	org.Keycloak
Gson	2.8.5	com.google.code.gson

Fuente: elaboración propia, realizado con Microsoft Word.

Tabla VIII. ***Librerías SIHUDA***

Nombre	*Versión*	*Proveedor*
Keycloak-core	4.1.0 Final	org.Keycloak
Keycloak-core-adapter	4.8.0 Final	org.Keycloak

Fuente: elaboración propia, realizado con Microsoft Word.

Tabla IX. **Librerías SINAF**

Nombre	*Versión*	*Proveedor*
Keycloak-core	4.1.0 Final	org.Keycloak
Keycloak-core-adapter	4.8.0 Final	org.Keycloak

Fuente: elaboración propia, realizado con Microsoft Word.

2.4.7. Integración de Keycloak en los portales web de la institución

Los cuatro portales webs ya existentes en el Instituto Nacional de Ciencias Forenses de Guatemala, están desarrollados bajo la misma tecnología, que es Java We*b*, XHTML, un gestor de paquetes que es Maven, por lo que comporten un comportamiento muy similar en la lógica de programación de inicio de sesión, por lo que el desarrollo para poderlos integrar a Keycloak fue muy similar.

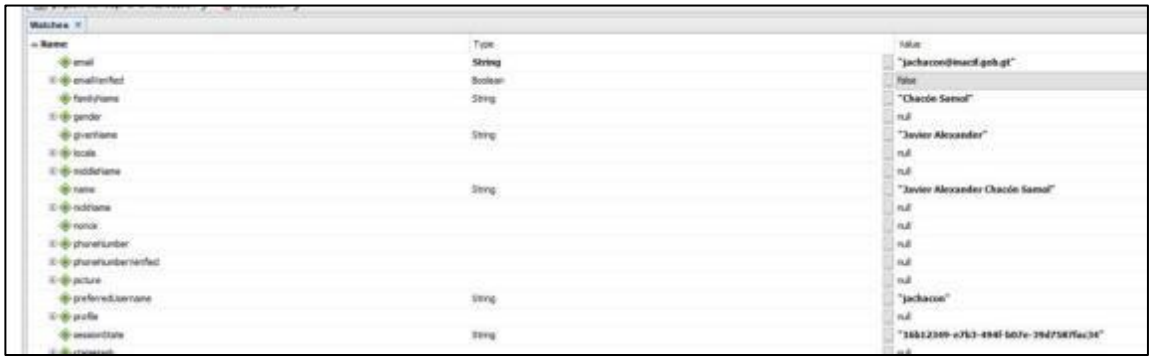
En cada uno de los portales, se buscó la clase en la que se maneja la lógica de programación de inicio de sesión, y se creó un método en el que se consume el servicio de Keycloak en cada portal, para sustituir de manera estratégica el código de inicio de sesión ya existente, lo que hace este código, consumir un *token* que provee Keyclo*ak* y obtener la información necesaria para seguir con el flujo ya existente de inicio de sesión. El *token* obtenido se descifra por medio del objeto AccesToken, este objeto se obtiene por medio de las librerías importadas de Keyclo*ak*.

Figura 23. **Código *Java***

```
public void authenticate() {

        try {
            Object sgContext =
FacesContext.getCurrentInstance().getExternalContext().getSessionMap().getOrDefault("org.keycloak.KeycloakSecuri
tyContext", null);
            String json = new Gson().toJson(sgContext);

            JsonObject gson = new Gson().fromJson(json, JsonObject.class);

            String tokenString = gson.get("tokenString").toString().replace("\"", "");

            AccessToken accessToken = RSATokenVerifier.create(tokenString).getToken();

            String nip = accessToken.getOtherClaims().get("employeeID").toString();
            String cui = accessToken.getOtherClaims().get("employeeNumber").toString();

          }

}
```

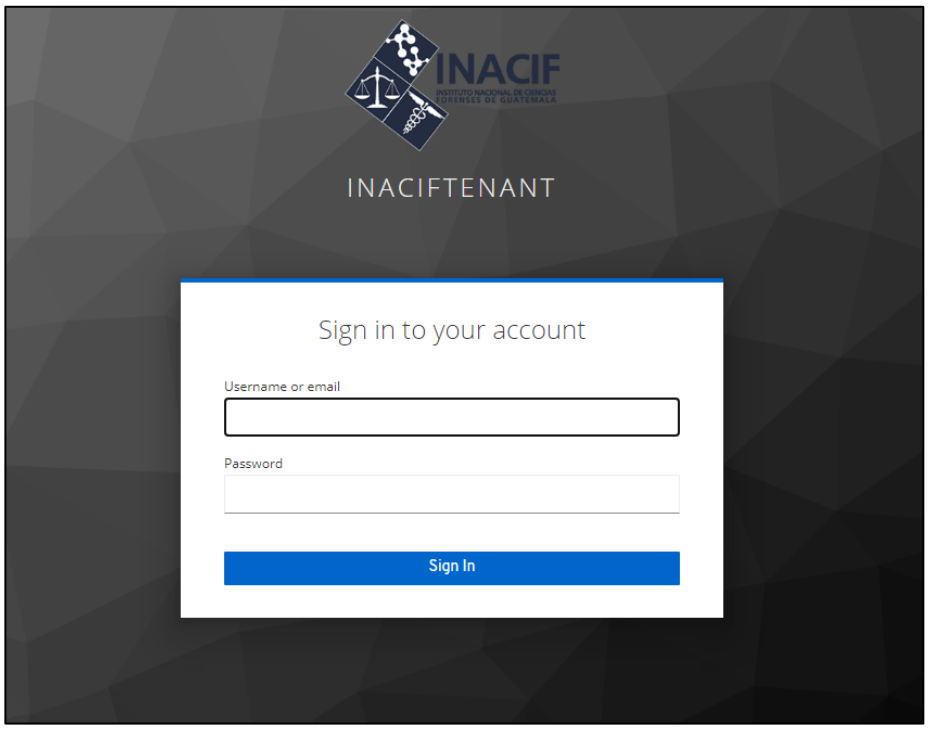
Fuente: elaboración propia, realizado con *Java*.

Figura 24. **Acces Token**



Fuente: elaboración propia, realizado con Neatbeans 8.2.

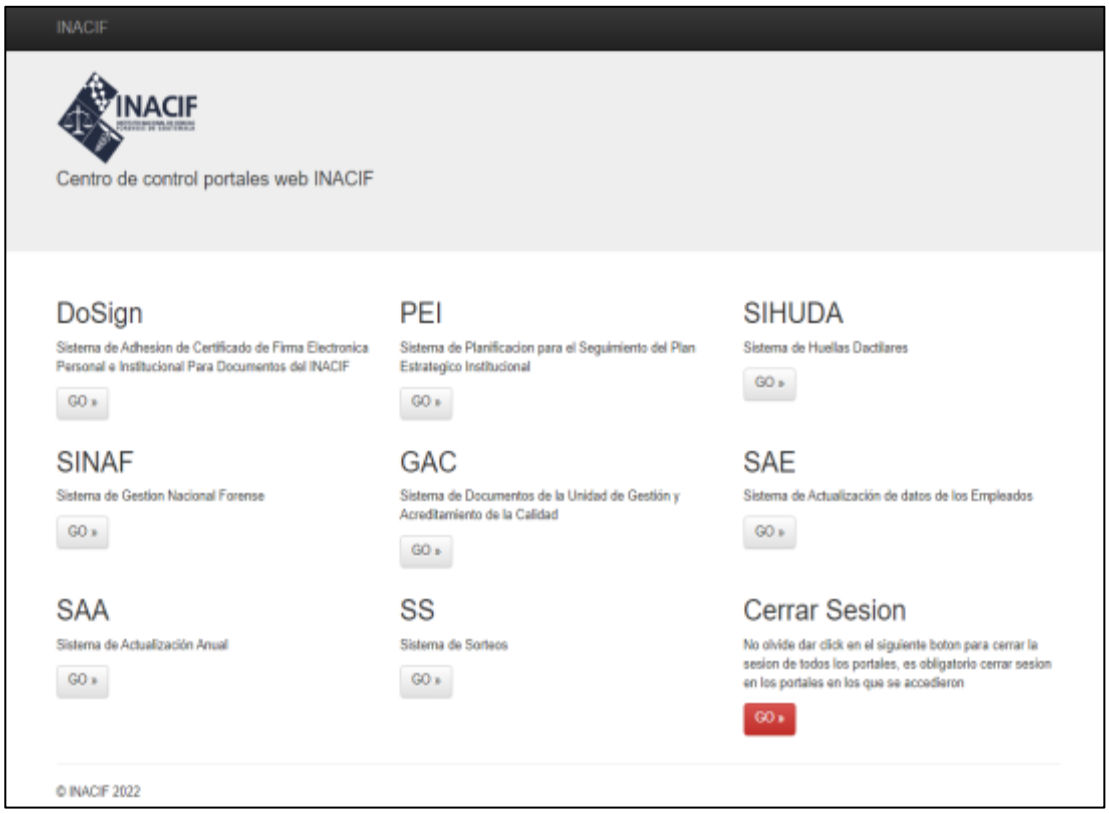
Figura 25. **Login Único**



Fuente: elaboración propia, realizado con Microsoft Word.

Se creó una página web, en la cual están contenidas las direcciones de los portales webs ya existentes, para que el usuario final acceda a esta página y de esta página se pueda redirigir a los portales webs en los que tiene acceso, esta página web está desplegada con *docker-compose* utilizando una imagen dockerizada de ningx.

Figura 26. **Menú de Aplicaciones**



Fuente: elaboración propia, realizado con Microsoft Word.

2.5. Costos del proyecto

Se incluyen aquellos valores representativos del proyecto.

Tabla X. **Costos**

Recursos	Cantidad	Costo (Q,)	Subtotal (Q,)
Desarrollador	1	Q 6 000,00 x 6 meses	Q 36 000,00
Asesor Personal	1	Q 3 000,00 x 6 meses	Q 18 000,00
Asesor INACIF	2	Q 5 000,00 x 6 meses	Q 30 000,00
Computadora portátil	1	Q 7 500,00	Q 7 500,00
Mouse	1	Q 500,00	Q 500,00
Teclado	1	Q 450,00	Q 450,00
Monitor	1	Q 950,00	Q 950,00
Internet	1	Q 300,00 x 6 meses	Q 1 800,00
Energía Eléctrica	1	Q 300,00 x 6 meses	Q 1 800,00
Servidor de desarrollo	1	Q 1 000,00 x 6 meses	Q 6 000,00
Servidor de autenticación	1	Q 500,00 x 6 meses	Q 3 000,00
Servidor de autenticación desarrollo	1	Q 500,00 x 6 meses	Q 3 000,00
Total	12	Q 109 000,00	Q 109 000,00

Fuente: elaboración propia, realizado con Microsoft Word.

2.6. Beneficios del proyecto

Serán aquellos resultados positivos post incorporación del proyecto diseñado para las necesidades presentes en INACIF.

2.6.1. Centralización de información

Se centraliza la información de los usuarios, sincronizando el servidor de autenticación con el Active Directory de la institución, evitando crear un usuario diferente por cada plataforma existente.

2.6.2. Mejor experiencia de usuario

Es necesario mejorar las condiciones de los usuarios finales quienes solo tendrían que administrar una credencial y así evitar duplicidad de funciones.

2.6.3. Sencillez de gestión

Se facilita la gestión de los usuarios en el sistema de autenticación único, porque Keycloak ofrece una interfaz sencilla de utilizar.

2.6.4. Escalabilidad

Al implementar un servidor de autenticación, se obtuvo un ambiente más escalable, porque es posible integrar cada aplicación nueva a este servidor, manejando siempre una credencial por cada usuario final.

3. FASE ENSEÑANZA APRENDIZAJE

3.1. Capacitación propuesta

Se realizó una capacitación, explicando cómo gestionar la herramienta de Keycloak, realizando una demostración con las tecnologías en las que se van a desarrollar las nuevas plataformas de la institución, en esta demostración se agregó un nuevo sistema de información basado en la web en Keycloak.

3.2. Material elaborado

Es la composición general de toda la propuesta desarrollada en la fase de investigación, que tratará de solucionar los problemas diarios en INACIF.

3.2.1. Servidor de desarrollo Keycloak

Debido a que se están desarrollando sistemas de información basados en la web para la institución, se optó por crear un servidor de desarrollo para ejecutar pruebas, y evitar cualquier tipo de manipulación al servidor de producción.

3.2.2. Servidor de producción de Keycloak

Este servidor es el que van a consumir las aplicaciones ya montadas en el ambiente final, o también conocido como ambiente de producción, este ambiente es bastante más delicado porque es el que contiene la información

oficial que está relacionada con la gestión de los usuarios y los sistemas de información basados en la web.

3.2.3. Código

Se elaboró el código fuente para integrar los 4 sistemas de información basados en la web de la institución al sistema de autenticación, también se elaboró el código necesario para poder crear instancias del servidor de *Keycloak*.

3.2.4. Demo

Es el código fuente, de un sistema de información basado en la web, con las tecnologías que quieren implementar en sus nuevos desarrollos web, el cual sirvió para demostrar que esas tecnologías son compatibles con el servidor de Keycloak.

4. RETROALIMENTACIÓN

4.1. Comentarios finales

Se utilizó *docker* para implementar el servidor de autenticación, debido a la versatilidad de esta tecnología, esto con la idea de que, si en un futuro se necesita realizar alguna mejora en la arquitectura del sistema, sea más sencillo migrar el servidor de autenticación; *docker* añade portabilidad en el despliegue de sus aplicaciones.

La configuración del servidor de autenticación no fue tan complicada, esto debido a que la documentación oficial de la herramienta de Keycloak está muy detallada.

Lo que realmente fue un reto fue integrar las aplicaciones web a la herramienta de Keycloak, esto debido a que las tecnologías sobre las que están desarrolladas son un poco antiguas, y no había suficiente información en la documentación oficial de Keycloak, sin embargo, el objetivo principal de usar Keycloak es que sea compatible con las plataformas que se irán añadiendo en la institución.

CONCLUSIONES

1. Se implementó Keycloak como servidor de autenticación, el cual es capaz de gestionar las sesiones de todos los usuarios de manera sencilla, la implementación se logró utilizando como base la tecnología de *docker*, esto debido a la portabilidad y versatilidad de esta.

2. En el sistema de autenticación implementado, se integraron las plataformas webs, que se encontraban en desarrollo, esto es porque la tecnología de Keycloa*k* es totalmente compatible con las tecnologías en las que se están desarrollando las nuevas plataformas webs de la institución.

3. Se integraron los 4 sistemas de información basados en la web ya existentes del Instituto Nacional de Ciencias Forenses de Guatemala en el sistema de autenticación único.

RECOMENDACIONES

1. Utilizar como guía, la documentación oficial de Keycloak, debido a que es la verificación verídica de la herramienta, es bastante completa.

2. Desarrollar los nuevos proyectos webs, sobre herramientas que sean totalmente compatibles con Keycloa*k*, ya que sería más fácil encontrar información en caso de cualquier inconveniente.

3. Configurar tecnologías como Kubernetes la cual proporcionará una mayor disponibilidad del servicio de Keycloak, puesto que se utilizó *docker* para la implementación del servidor de autenticación, se puede ir un paso más adelante.

BIBLIOGRAFÍA

1. INACIF, (2020). *Historia INACIF*. Guatemala. Recuperado de https://www.inacif.gob.gt/index.php/inacif/historia.

2. Jetbreains. (2020). *Publicación OAuth2.0.* República Checoslovaka. Recuperado de https://www.jetbrains.com/help/youtrack/devportal/OAuth-authorization-in-youtrack.html.

3. *Keycloak*. (2020). *Documentación oficial*. Estados Unidos. Recuperado de https://www.*Keycloak*.org/documentation.

4. OAuth0, (2021). *Documentación oficial*. Estados Unidos. Recuperado de https://auth0.com/docs/authenticate/single-sign-on.